Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (currently amended) A method of inter-area rekeying of encryption keys in secure mobile multicast communications, comprising:

at a Domain Group Controller Key Server (Domain GCKS):

distributing Traffic Encryption Keys (TEK) to a plurality of local Group Controller Key Servers (local GCKS) serving respective group key management areas, wherein said local Group Controller Key Servers forward said Traffic Encryption Keys, encrypted using Key Encryption Keys (KEK_i, KEK_j) that are specific to the respective local Group Controller Key Server (local $GCKS_i$, $GCKS_j$), to group members situated in the respective group key management areas, and wherein said local Group Controller Key Servers ($GCKS_i$, $GCKS_j$) constitute Extra Key Owner Lists ($EKOL_i$, $EKOL_j$) for said group key management areas ($area_i$, $area_j$) that distinguish group members (MM_i, MM_j) possessing Key Encryption Keys (KEK_i, KEK_j) and situated in the corresponding group key management area ($area_i$, $area_j$) from group members (MM_{ij}) possessing Key Encryption Keys (KEK_i) that were situated in the corresponding group key management area ($area_i$) but are visiting another area ($area_j$);

forwarding said Traffic Encryption Keys (TEK) to group members (MM_{ij}) visiting the respective group key management areas ($area_j$) encrypted using a Visitor Encryption Key (VEK_j) that is specific to the respective local Group Controller Key Server ($GCKS_j$) and is different from said Key Encryption Key (KEK_j); and

sending a new Visitor Encryption Key (VEK_j) to a mobile member (MM_{ij}) arriving in the corresponding group key management area ($area_j$) ~~if there is no other mobile member (MM_{ij}) situated in the corresponding group key management area ($area_j$) and if~~ when a current Visitor Encryption Key (VEK_j) exists ~~that~~ and the current Visitor Encryption Key (VEK_j) has already been used to encrypt a previous Traffic Encryption Key (TEK), wherein only one new VEK_j value is derived regardless of the number of new mobile members that enter the group key management area ($area_j$).

2. (previously presented) A method as claimed in claim 1, further comprising rekeying said Traffic Encryption Keys (TEK) after rekeying said Key Encryption Key (KEK_i, KEK_j).

3. (previously presented) A method as claimed in claim 1, wherein said local Group Controller Key Servers ($GCKS_i$, $GCKS_j$) rekey a Key Encryption Key (KEK_i, KEK_j) by a process comprising sending a new Key Encryption Key (KEK_i, KEK_j) to current group members encrypted using the current Key Encryption Key (KEK_i, KEK_j) and to mobile members using the Visitor Encryption Key (VEK_i, VEK_j).

4. (previously presented) A method as claimed in claim 1, wherein said local Group Controller Key Server $GCKS_i$ sends the Visitor Encryption Key (VEK_i) rather than the Key Encryption Key (KEK_i) to new members joining the group via $area_i$.

5. (previously presented) A method as claimed in claim 3, wherein said local Group Controller Key Servers ($GCKS_i$, $GCKS_j$) rekey a Key Encryption Key (KEK_i, KEK_j) by a process comprising sending said new Key Encryption Key (KEK_i, KEK_j) selectively to existing group members situated in the corresponding group key management area ($area_i$, $area_j$).

6. (previously presented) A method as claimed in claim 3, wherein said local Group Controller Key Servers ($GCKS_i$, $GCKS_j$) rekey a Key Encryption Key (KEK_i, KEK_j) by a process comprising sending said new Key Encryption Key (KEK_i, KEK_j) to existing group members using multicast messages and to said visiting mobile members over a different secure channel.

7. (previously presented) A method as claimed in claim 3, wherein rekeying a Key Encryption Key (KEK_i, KEK_j) comprises said local Group Controller Key Servers ($GCKS_i$, $GCKS_j$) sending a new Key Encryption Key (KEK_i, KEK_j) selectively to current group members currently situated in the corresponding group key management areas ($area_i$, $area_j$).

8. (previously presented) A method as claimed in claim 3 further comprising constituting Visitor Key Owner Lists ($VKOL_i$, $VKOL_j$) for said group key management areas ($area_i$, $area_j$) that distinguish group members (MM_i, MM_j) possessing Visitor Encryption Keys (VEK_i, VEK_j) and situated in the corresponding group key management area ($area_i$, $area_j$)

from group members (MM_{ij}) possessing Visitor Encryption Keys (VEK_i) that were situated in the corresponding group key management area ($area_i$) but are visiting another area ($area_j$).

9. (previously presented) A method as claimed in claim 8_x wherein said Extra Key Owner Lists ($EKOL_i$, $EKOL_j$) and said Visitor Key Owner Lists ($VKOL_i$, $VKOL_j$) comprise lists of the group members $(MM_{ij})_x$ possessing Key Encryption Keys (KEK_i), ~~respectively~~ and Visitor Encryption Keys (VEK_i, VEK_j) respectively, that were situated in the corresponding group key management area ($area_i$) but are visiting another area ($area_j$).

10. (previously presented) A method as claimed in claim 1, wherein a group member (MM_{ij}) that was visiting another group key management area ($area_j$) returns to an area ($area_i$) for which it possesses a corresponding Key Encryption Key (KEK_i) or Visitor Encryption Key (VEK_i) before expiry of a validity period set by the corresponding Group Controller Key Server ($GCKS_i$) without said corresponding Group Controller Key Server ($GCKS_i$) rekeying said Key Encryption Key (KEK_i).